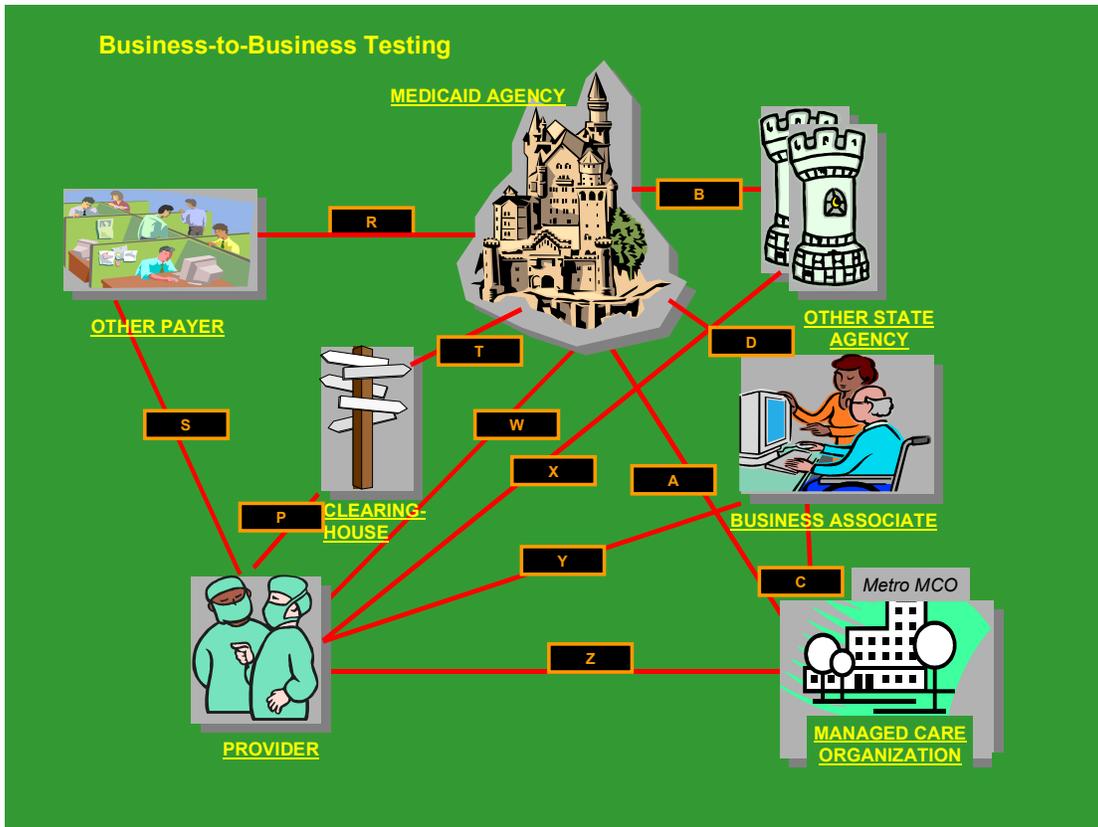


CENTERS FOR MEDICARE & MEDICAID SERVICES



TESTING! TESTING!
Do You Read Me?



ROAD MAPS TO HIPAA COMPLIANCE VOLUME 2, MAP 3



February 20, 2002

This paper is the third in the year 2 series of the Centers for Medicare & Medicaid Services (CMS) white paper publications. Year 2 publications are dedicated to practical, how-to approaches to comply with HIPAA requirements.

TESTING! TESTING! DO YOU READ ME?

PURPOSE OF THE PAPER



The Centers for Medicare & Medicaid Services (CMS) white paper on testing seeks to clarify the different types and levels of testing required for HIPAA implementation, broadcast the magnitude of this endeavor, and provide guidance in survival tactics for State Medicaid agencies and their data trading partners.

In the past, State Medicaid agencies have been able to manage the testing with providers who agree to do business via electronic transactions. These tests have focused on claims submission or the implementation of a new eligibility verification system.

With HIPAA, *the world changes*. Even with a year's extension of the deadline for HIPAA (based on the submission of the required Compliance Plan) most States will be burdened with the demands of increased testing. States rallied to the testing challenges of the Year 2000, but with HIPAA, internal and external testing requirements will greatly increase, not only in number, but in complexity as well. For example:

- ❑ Currently most States issue paper vouchers to accompany electronic fund transfers or paper checks, but HIPAA requires the capability to produce a more complex accounting transaction, the electronic 835.
- ❑ Where payers now conduct prior authorization and claim status inquiry primarily by telephone and fax, they will soon be required to implement entirely new transaction formats and accompanying business processes.
- ❑ The typical eligibility verification system (EVS) installs a terminal in the provider's office. Testing the EVS is a simple process. While use of the terminal reduces the potential for erroneous claim submissions, it does not require the provider to demonstrate the ability to receive the standard eligibility response transaction (the electronic 271).

Medicaid agencies and their data trading partners have never before experienced the intensity and complexity of testing that HIPAA implementation requires.

In contrast to these examples, all the HIPAA transactions must be tested with multiple trading partners as well as in-house. Complex and rigorous testing is the key to insuring success whereby the standards mandated by HIPAA result in overall improvement of business processes.

TOPICS COVERED IN THIS PAPER



This paper covers the following material:

- Vocabulary of Testing
- Testing Zones
- Testing the Translator
- Internal Medicaid Agency Systems Testing
- Business-to-Business Testing

VOCABULARY TEST

The following key words and terms are used in this paper. They are presented here in alphabetical order. Later in the paper each of these types of testing is described in more detail.

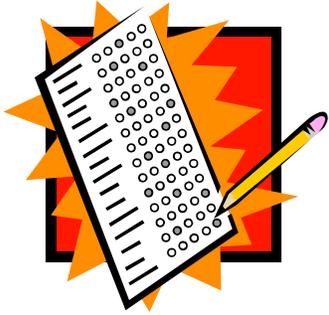
Blanket Approval—This is a testing policy that the Medicaid agency or a clearinghouse could establish for multiple provider groups or individual providers who use a specific software vendor’s product to generate and transmit the transactions. A “blanket approval” requires a minimum number of providers who must generate and transmit the transaction with a minimum number of errors in the batch. Blanket approval is given separately for each transaction.

Business-to-Business Testing—Business-to-Business testing refers to the body of tests conducted between two data trading partners who exchange HIPAA standard transactions to determine the readiness of these entities to “go live”.

Internal Medicaid Agency Systems Testing—These tests ensure that the incoming transactions, once converted by the translator, can be successfully processed end-to-end throughout the Medicaid Management Information System (MMIS) and its off-shoots, e.g., data warehouse, fraud detection application, third party recovery process, and other reporting systems, and that outgoing transactions can be successfully produced and exported. Internal end-to-end testing assumes that all HIPAA-related changes to the MMIS, such as remediation of logic needed to generate a compliant remittance advice (835), have already been thoroughly tested.



Levels of Testing—The different types of testing contain within them different *levels* of testing. For example, you can validate the correct formatting of a received X12N transaction (Level 1) and in addition you can validate correct data content in the fields (Level 2). Levels of testing are defined in more detail in the sections that follow.



Product Appraisal—Product appraisal is a service that can be purchased to provide approval or endorsement of a specific solution product as part of an organization’s implementation plan. Information Technology Research groups, such as the Gartner Group, provide product appraisals for their subscribers.

Transaction Certification Testing—Transaction Certification is an independent “stamp of approval” that the translator product or the transaction intake and output applications correctly implement the requirements of each Implementation Guide and are capable of receiving and sending compliant transactions. Transaction Certification does not validate the Business-to-Business data exchanges between data exchange partners, nor does it validate the internal processing of the MMIS, or other transaction processing system.

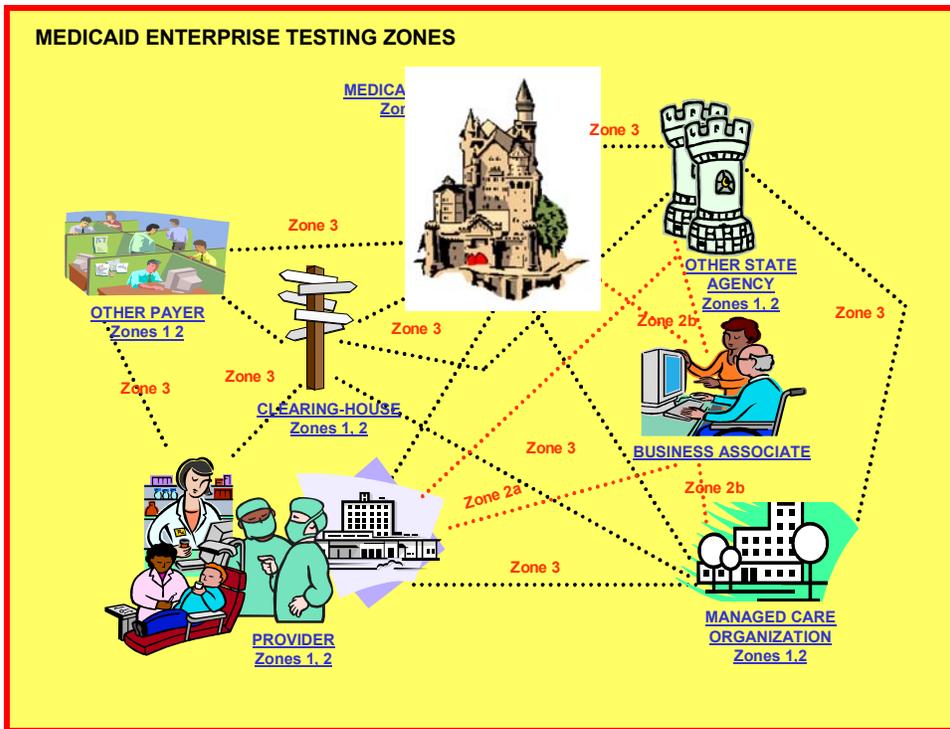
Translator Installation Testing—Even if the translator has been “factory certified”, once it is installed in the entity’s system, it will need to be tested to validate all the mapping rules and other functionality the agency requires of the product.



TESTING ZONES

The Medicaid enterprise presents a daunting landscape in which the types of testing and the levels of testing need to occur. Each covered entity is responsible for its own internal testing, however, testing is not complete until each entity has tested with its data trading partners. A look at the Medicaid enterprise as illustrated in the Medicaid HIPAA-Compliant Concept Model (MHCCM) shows a complex web of relationships. The enterprise is made up of entities that continuously exchange different types of data. Many transactions elicit a response transaction. Despite the HIPAA compliance deadline extension, it might not be possible for each individual entity to test every sending and receiving transaction with every other party.

The Medicaid enterprise test zones are illustrated in the following diagram.

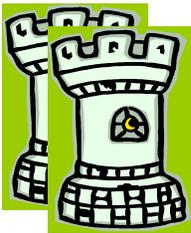


Zone 1 = Translator Testing and Certification
Zone 2 = Internal Testing
 (2a, 2b=Testing with Business Associate)
Zone 3 = Business-to-Business Testing

The major testing zones based on the Medicaid Enterprise model above are:

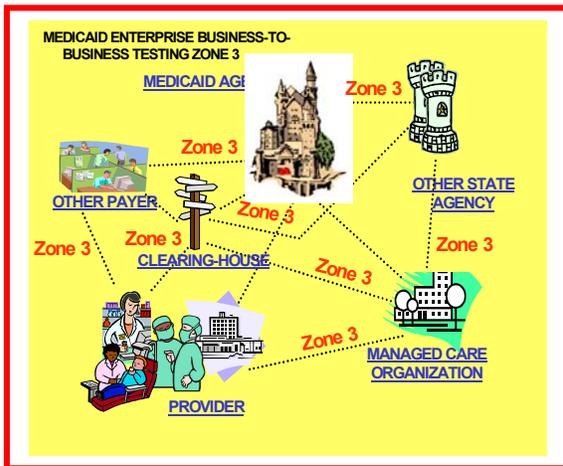
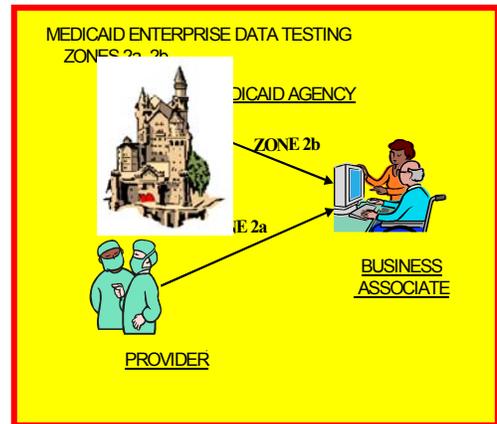
Test Zone	Required Tests
Zone 1: Translator testing and certification—Each covered entity must test its own compliance.	Ideally, the translator has been “factory certified” prior to installation. After installation, the translator product or application must demonstrate its ability to receive and send HIPAA compliant transactions and to interface with the client’s processing systems.
Zone 2: Internal application testing—Each entity must test its own business systems.	All entities need to conduct internal testing of their applications and systems. Can the modified application programs produce the same pre-HIPAA results using the new standard data? Zone 2 also includes testing that is required between the covered entity and its business associate. The business associate conducts business on behalf of the covered entity (see 2a and 2b).
<ul style="list-style-type: none"> Zone 2a: Provider to Business Associate (e.g., a Practice Management System Vendor) 	Providers may lease back office software, contract for this service, or support it on their own. In all cases, the provider’s practice management system should be able to produce and receive standard HIPAA transactions. Alternatively, providers or their vendors can use a clearinghouse.

Test Zone	Required Tests
<ul style="list-style-type: none"> Zone 2b: Health Plan to Business Associate (e.g., Medicaid fiscal agents, enrollment brokers) 	The Medicaid agency by law must be able to accept standard transactions and transmit standard transactions. The agency's business associates, especially fiscal agents, data warehouse contractors, prior authorization entities, eligibility verification services, and others must demonstrate HIPAA-compliant capability.
Zone 3: Business-to-Business testing—From one data trading partner to another	All data exchange partners must demonstrate they can exchange compliant data with one another.



In Zone 1 (test the translator) and Zone 2, (testing of the internal systems), each entity that installs a translator and/or changes its internal systems to meet HIPAA compliance requirements is expected to perform its own validation of these implementation strategies. For example, the “Other State Agency”, e.g., a Department of Mental Health, may install a translator and modify its applications. It is that agency’s responsibility to test these changes.

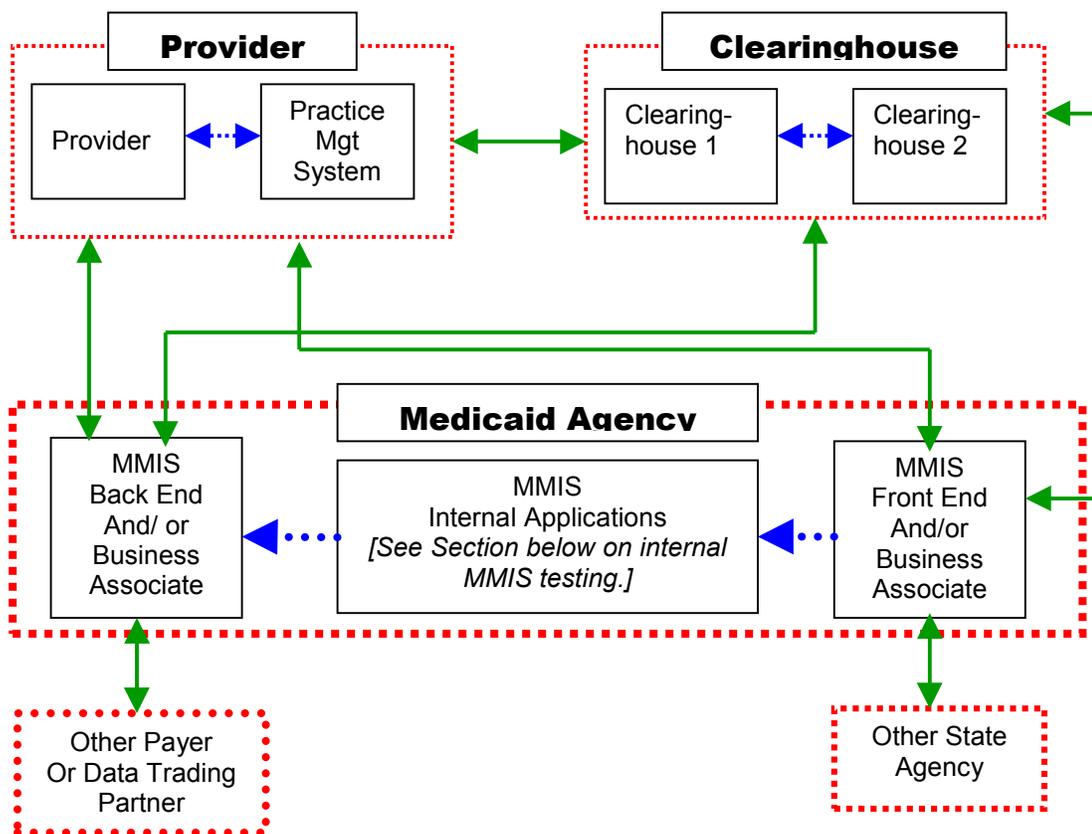
Zone 2a and 2b testing is an extension of internal testing. The covered entity requires its business associates to establish the readiness and compliance of the applications they operate for the covered entity. In this example, the business associates, e.g., the Medicaid agency’s fiscal agent or the provider’s system vendor must achieve and maintain HIPAA compliance for the entities they serve.



Zone 3 is Business-to-Business testing, the major challenge for all of the participants. The coordination of these activities requires awareness on the part of all, and leadership from the Medicaid agency. Each covered entity could have its own schedule of implementing and testing each transaction. However, to conduct Business-to-Business testing, all parties have to be ready to test the same transaction at the same time.

Ideas to reduce the tension and confusion, the volume of tests, and the costs are presented in sections below. The following chart puts all the pieces together.

TESTING ZONES



LEGEND:

- Broken line red box = Internal Testing Zones 1, 2
- Broken line blue arrow = Internal Testing Zone 2
- Solid green arrow = Business-to-Business Testing Zone 3



The Year 2000 (Y2K) provides a model for preparation for HIPAA implementation. In Y2K testing, States had to deal with the same three Zones. (Zone 1 was mainly limited to date conversion algorithms). Lessons learned and documents archived from Y2K provide a foundation for HIPAA implementation. However, as stressed in this paper, the challenge of HIPAA compliance far exceeds the demands of Y2K in terms of volume and types of transactions, fields to be tested, levels of testing, complexity of testing, Business-to-Business testing, and internal testing.

In the following sections of this paper we will focus on more detail regarding the Testing Zones. First is Zone 1, Testing the Translator.

TESTING THE TRANSLATOR (TEST ZONE 1)

Testing Zone 1 focuses on the covered entity's ability to send and receive mandated transactions in strict adherence to the requirements of the Implementation Guides. Each electronic sender and receiver must have the ability to convert from and to X12N formatting and control elements, and for some time into the future, from and to local codes. Technically, a translator COTS product is not needed but there must be some form of translator application. Zone 1 covers testing of the compliance of the translator application or product. Each entity needs to demonstrate its compliance.

Aids for Zone 1 Testing

Possible options include:

- ❑ *Traditional testing*—The Medicaid agency creates test transactions based on the directives of the Implementation Guides and the results of their data content and code set mapping. The agency could make the test transactions available to their data trading partners.
- ❑ *Independent Verification and Validation*—The agency contracts with an independent testing organization. The IV&V organization creates and applies test data.
- ❑ *Transaction Compliance Certification*—The agency subscribes to an independent certification service. The service uses its test cases to test the transaction intake and output functions. If the service is recognized by the health care industry, it can apply a “Good Housekeeping” stamp of approval on customers who pass the test.
- ❑ *Product appraisal*—The Medicaid agency obtains the services of a technology research group which provides a high level “blessing” of the translator product based on the product's performance in general, but not necessarily *in situ* as installed at the agency.

A WEDI/SNIP Work Group¹ has defined a number of test levels for the health care industry to use in determining compliance of mandated transactions. The tests at each level can be applied independently; however, the more levels that are applied, the greater the confidence that the processor will be compliant. Levels 1 and 2 represent the bare minimum of testing for compliance. Any sender/receiver system can apply these tests. The levels of testing are also appropriate to all the testing options listed above. The covered entity has to decide both the testing strategy and the level of testing it will conduct.

SNIP Levels Of Transaction Compliance Testing

SNIP has produced a white paper on *Testing and Certification* that describes recommended solutions associated with HIPAA transaction compliance. The draft

¹ SNIP Transactions Work Group/Testing Sub Work Group, white paper entitled *Testing and Certification*, currently in draft version, available at the wedi.org Web site.

version of the SNIP paper, page 5, recommends six levels of testing as reported below. Previous compliance testing models have only included the first two levels.

The following are the SNIP levels of testing to achieve compliance certification.

- Level 1: *Integrity testing* – Testing for valid segments, segment order, element attributes, numeric values in numeric data elements, X12 syntax, and compliance with X12 rules. This process tests the fundamental formatting and control elements of the X12N envelope and internal structure.



- Level 2: *Requirement testing* – Testing for HIPAA implementation-guide-specific requirements, such as repeat counts, used and not used codes, elements and segments, required or intra-segment situational data elements, non-medical code sets as laid out in the Implementation Guide.

Tests the code value specified in the guide for that transaction (as opposed to external code sets).

- Level 3: *Balancing* – Testing for balanced field totals, record or segment counts, financial balancing of summary fields.
- Level 4: *Situation testing* – Testing of specific inter-segment situations described in the HIPAA Implementation Guides, including the validation of situational fields given values or situations present elsewhere in the file. For Levels 4-6, Transaction Certification becomes more Trading Partner specific – and Trading Partners have some discretion in how the HIPAA compliant transactions will be conducted. Examples of Level 4 testing are:

- A Medicaid payer who may require the use of its Medicaid provider numbers until the National Provider Identifier Standards are effective.
- A payer’s requirement that a home health provider use an 837 professional rather than an 837 institutional claim format for submission.
- Level 4 testing of Conditional Situations, Code Sets, and Product Types or Types of Service are “line of business” specific, and must comply within those parameters. For example, ambulance providers will need capacity to submit specific segments relating to their line of business and receivers of transactions for ambulance providers will likewise need the capacity to respond.
- Code Set validation ensures that the code usage “makes sense” for any particular transaction between given senders and receivers. For example, CDT codes, even if valid, are not appropriate on an 837 professional claim.
- Other Business Rules for Medicaid/Medicare/Worker Compensation, e.g., the requirement that a signed consent form accompanies all hysterectomy and sterilization claims or that a worker’s compensation claim be preceded with a First Report of Injury Transaction.

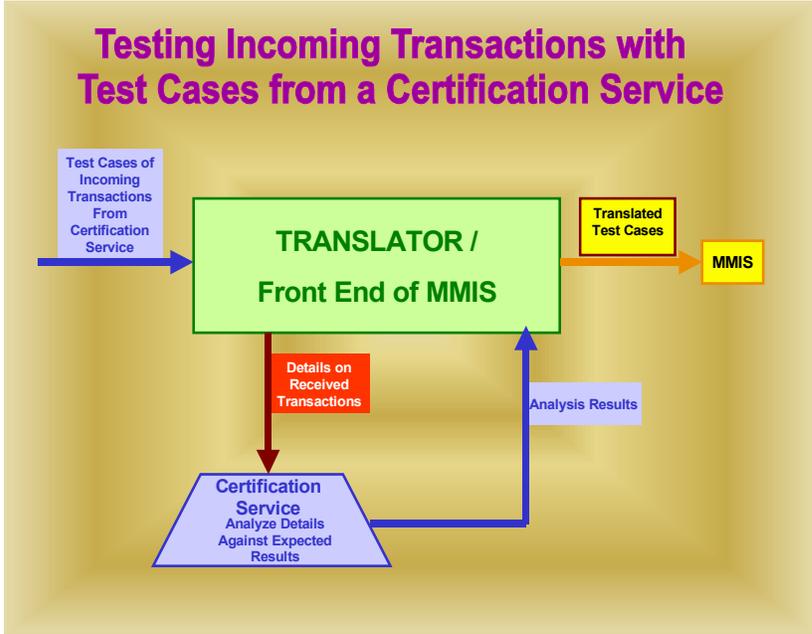
- The 270/271 will require that payers establish and providers be capable of and willing to conduct eligibility verification to a specified level of information: either general, categorical or benefit level and agree on the data elements that must be correctly submitted. Output to the provider will depend on the level of request the payer will allow and the payers’ rules for error tolerance – i.e., the submitter can’t “go fishing.”
- Level 5: *Code Set testing* – Testing for valid implementation-guide-specific code set values, makes sure the usage is appropriate for any particular transaction. Validates external code sets, e.g. CPT, HCPCS, ICD9, CDT, NDC, remittance advice codes, etc., and their appropriate use within the transaction. Level 5 would ensure that senders and receivers are matched for telecommunications, volume, scheduling and other transactional logistics.
- 
- Level 6: *Product Types/Types of Service testing* – Particular testing required by certain health care specialties, e.g., ambulance, chiropractic, home health, durable medical equipment, and other specialties each of which has its own special code requirements.

Compliance Certification

In order to adequately test HIPAA requirements, health plans will have to test with a large number of transaction submitters, and providers will have to test with many health plans. It is expected that this testing will be more demanding than any ever before experienced by the health care industry. The use of a third party² to certify compliance with HIPAA Implementation Guides can reduce the timeframe and cost involved in testing by substantial elimination of point-to-point testing. This cost reduction is highest when significant numbers of data trading partners, e.g., providers and clearinghouses, have also used a certification service. This results in reduction of the cost of implementation for both providers and payers.

Diagrams on the next pages illustrate the use of a compliance testing service.

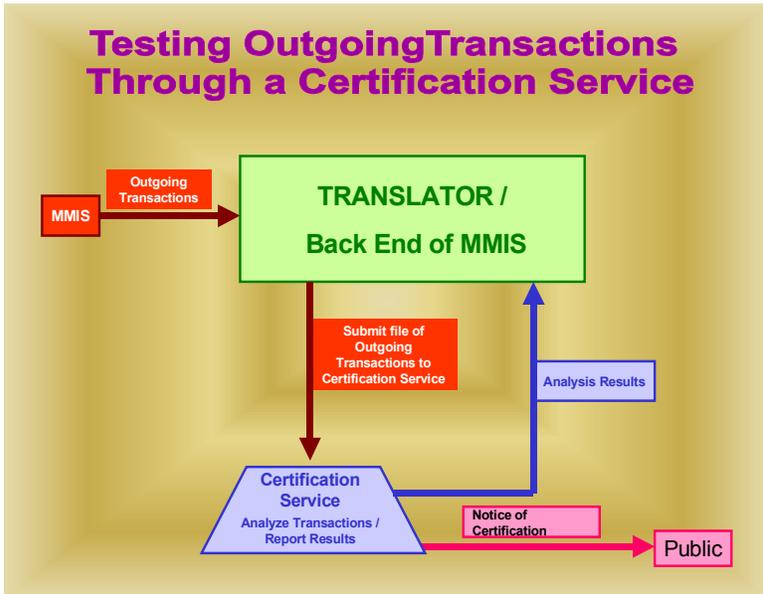
² For a list of compliance testing products and services, see the WEDI SNIP paper, “Testing and Certification: A White-Paper Describing the Recommended Solutions Associated with Compliance Certification of the HIPAA Transactions”, Appendix B. NOTE: *This information is cited by CMS as a reference source only and does not constitute a recommendation or endorsement of any kind.*



In the first diagram, the certification service supplies the test files, the client runs the tests, and sends the results to the service. The service analyzes the results and declares the client “certified” or not.

Certification can be in the form of a certificate and public notice.

For outbound transaction testing, the client can produce the transactions, submit them to the translator, create the outbound compliant formats, send these to the certification service, and receive the results of the analysis, i.e., “certified” or not. Certification increases the confidence of the payer and its providers that the payer is compliant.



Along with the benefits of compliance certification there are also some limitations:

1. Compliance certification is valid only for the time in which it is conducted.

Changes to X12N format and data content need to be retested. Changes to the transaction intake and output programs have a ripple effect and trigger a new round of compliance testing.

2. A translator may be “factory certified” but would still require certification at each installation because its functionality at each new site may change.
3. Compliance certification applies to the translator or sending and receiving applications only. It does not apply to the actual transmission of transactions

(business-to-business) or to the internal processing applications. However, it can decrease the levels of testing required in these other tests.

Even if the sender and receiver are certified, errors can still occur. For example, if the resulting transactions have currency fields that moved the decimal one unit to the right or left, a major disruption could ensue. There needs to be some form of “end-to-end” testing among all senders and receivers, or sequential testing that ensures that the next system into which a transaction moves, both on its inbound and outbound journey, yields expected results for some percentage of trading partners. (This might be handled as part of a blanket approval.)

Note: certification testing does not verify the entity’s internal systems and does not test the actual transmission between two data trading partners. Certification testing says: “This entity can receive and/or send HIPAA compliant standard transactions and data sets.”

Testing the Translator Installation

Even if the translator software has been “factory certified” as complying in every detail with the requirements of the Implementation Guides, it must still be tested again once it is installed in the organization’s system. First of all, “factory certification” only assures that the product contains the format and code set rules of the guides. Once installed, it must be tested to verify that the mapping of the client’s data to the X12N fields is accurate and that additional functions provided by the translator are correctly performed. The additional functions include conversion of standard to local codes where possible and when necessary, and stripping and storing of data not needed for transaction processing, but required to construct an outbound transaction. The following table summarizes key tests for the translator.

TRANSLATOR FUNCTIONS
<input type="checkbox"/> Mapping — Ensure all data content is addressed appropriately.
<input type="checkbox"/> Rules — Test logic associated with each business rule for content being mapped.
<input type="checkbox"/> Strip and Store—Test the capability of the installed translator to strip and store the data fields needed for the outbound transaction, but not needed for the internal processing record.
<input type="checkbox"/> Acknowledgments — Set yourself up as a sender and receiver. Assure that any acknowledgments are being produced appropriately and completely.
<input type="checkbox"/> Inbound and Outbound Content — All inbound and outbound transaction content must be verified. This test ensures compliance. Use translator’s ability to check syntax and transaction requirements.
<input type="checkbox"/> Event Handling — Test all event-handling routines (triggers, error handling, and host communications).

- ❑ Logging —Keeps track of all inbound and outbound transactions and transaction status. All logging functions must be tested and verified.
- ❑ Throughput — Test translator ability to process expected transaction volume especially for peak volumes. Throughput is expressed in volume of claims per second, eligibility requests per second, and responses per second.

Testing the translator product or application is an ongoing function. Test results are valid for a point in time when the test is conducted. Unfortunately, the standards will evolve and more will be added, e.g., attachments, acknowledgments,



“La donna e mobile...”
“Chaaange, chaaaange,
chaaange”

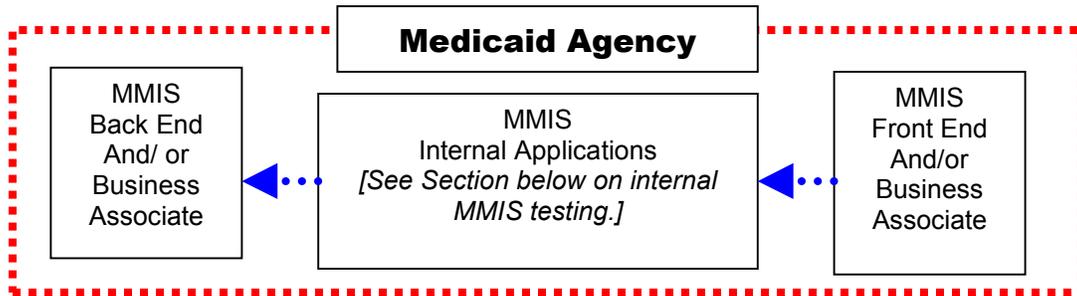
new standards, and new uses of existing standards. New versions of existing standards and new codes will be approved by the

Designated Standards Maintenance

Organizations (DSMO). All such changes that are approved by the Department of Health and Human Services (DHHS) must be implemented by the covered entities. Each time, the translator application must be updated and retested. In addition, the agency may find errors in its data mapping or new strip and store requirements, causing additional modifications to the translator function. For these reasons, the

Medicaid agency should invest in a long-term testing strategy that will always be available when needed. The next big area for testing is Zone 2, Internal Testing.

INTERNAL MEDICAID AGENCY SYSTEMS TESTING—(TEST ZONE 2)



The next testing zone covered in this paper is internal Medicaid Agency Systems testing (Zone 2). The following are some of the considerations for States as they plan the testing of the entire MMIS including its virtual components. The following tables highlight testing requirements for the Adjudication System, the Reporting Systems, and the testing methodology in general.

Testing the adjudication processes is particularly difficult for States with legacy systems in which editing and pricing logic is driven by hard-coded local codes (such as Category of Service, Provider Type, location, type of service, and others). Testing requirements will vary depending on the State's decision to convert as many incoming standard codes to local codes as possible *versus* modifying the adjudication applications and databases to bring in the new standard codes and replace the local codes. Testing will also differ if the State is moving from a paper process to an electronic process *versus* an established pre-HIPAA electronic process.

ADJUDICATION SYSTEM TESTING	
❑	<i>Edits and Associated Logic</i> —Edit logic will significantly change because new standard codes will replace local codes embedded in system logic, e.g., national remittance reason codes, claim status codes, elimination of local service codes, provider taxonomy, and many other code sets.
❑	<i>Front End System Edits</i> —Some of these may be handled by the translator, others by the adjudication system. These are first level edits such as valid provider ID, valid recipient ID, acceptable date of service.
❑	<i>Logic Edits</i> —Edits like diagnosis/procedure invalid for sex will be impacted by local code elimination.
❑	<i>Pricing Edits</i> —Data content, local code elimination, and new COB mechanisms may have caused changes in pricing logic. Verify that edits are correct and reference files are updated appropriately.
❑	<i>History Edits</i> —Any history conversions or crosswalk mechanisms put in place to handle value differences must be verified. (Example: Test Duplicate Check edits prior to and after HIPAA Implementation)
❑	<i>File integrity</i> —Reference, recipient, claims history, and provider files will be impacted with changes due to HIPAA. Test all code conversion tables. <ul style="list-style-type: none"> • Key fields—Assure file/table keys can handle identifiers, new

ADJUDICATION SYSTEM TESTING

- procedures/modifiers. Verify content. Ensure all data is being captured.
- I/O—Verify data can be accessed and written correctly
 - NOTE: Testing of claims/encounter history files will differ depending on the State’s decision to switch to new standard codes or to retain legacy codes. Either way, testing must match the State’s strategy for handling of data.
- *Payment Systems*—Payment processes are affected by local code elimination, new remittance reasons, and monetary field length differences.
- Overflow/Underflow—Test truncation and all summation routines, e.g., multiplier functions such as funding computations.
 - Remittance Reasons—This is an entirely new code set and must be thoroughly tested.
 - Internal Auditing—Include auditing staff in test verification. Assure audit mechanisms work as expected.
- *Reference Files*—Reference Files will change due to local code elimination, edits, and identifier changes. All conversion mechanisms and cross-walking mechanisms must be verified.

Testing the front-end adjudication system functions is the first step. Next, all reporting systems must receive the same level of testing. Reporting systems are totally dependent on the quality of data they receive. The Management and Reporting Subsystem (MARS), the Surveillance and Utilization Review Subsystem (SURS), the State’s files for the Medicaid Statistical Information System (MSIS), and the Data Warehouse and all of its decision support capability must be able to function at full capacity.

All local code issues must be resolved. Careful testing of the output of these systems is critical to the health of the Medicaid agency. Reporting systems require extensive testing since all content has been affected by adoption of HIPAA standard code sets (new codes and missing local codes such as category of service). This will be the case whether or not the State has opted to convert as many standard codes as possible to the legacy codes, or has changed internal databases and applications to adapt to the standard codes. In the latter case there is likely to be more testing required. CMS recommends States move as quickly as possible to the use of the standard codes throughout the MMIS. It is recommended that any new system implemented as “HIPAA-compliant” should include the requirement that only standard codes will be used throughout.

“One of the benefits of Administrative Simplification is that at some time in the future, providers and payers will be using the same standard code sets. Therefore, we encourage all States to move as quickly as possible to adopt the standard codes in all MMIS applications and files. All new MMIS systems should use standard codes from HIPAA-covered transactions.”

***- Rachel Block
Director, Financial Systems and Quality Group
Center for Medicaid and State Operations***

TESTING OF REPORTING SYSTEMS: MARS, SURS, MSIS, DATA WAREHOUSE, AND OTHER REPORTING

- ❑ Service Classification—Local codes elimination, provider taxonomy (specialty codes, provider type, service type) and any new data content will have an impact on service classification.
- ❑ Numeric underflow/overflow—Monetary field size changes may have impacted summary totals.
- ❑ Database conversions—Changes in content in adjudicated claim files/tables, recipient tables, provider tables will impact reporting.
- ❑ Data warehouse—The data warehouse environment will be impacted by operational system changes in content, service classification, local code elimination, identifier changes (NPI), and summary operations.
- ❑ Table load processes—Test for content, test crosswalk and conversion mechanisms, table structure changes.
- ❑ Key integrity—Changes in identifiers, local codes and other content carried as key table elements must be validated and access based on keys must be tested.
- ❑ Rule integrity—Test all triggers, event procedures and object references at the database and Executive Information System, Decision Support System, and other application levels.
- ❑ Access log—All logging mechanisms and alarms are tested and event reporting mechanisms must work.

HIPAA changes impact the entire Medicaid operational and reporting environments and require incremental and iterative testing procedures. Changes will cause system imbalances that may be far-reaching, extending into system areas that have not been changed. The following outlines a testing methodology to cover all the bases.

TESTING METHODOLOGY

- ❑ Existing testing procedures should be reviewed and modified to accommodate all levels of unit and system testing requirements. Test teams should be utilized. Plan for these resources.
- ❑ Modify and test the systems in small increments. Test region should contain current production environment plus changed portion.
- ❑ Increase the restore capability to twice its current level (if system contains two versions in archive, increase to four versions).
- ❑ Retest entire system for each incremental development effort. Parallel test production and test environment and compare and validate results.
- ❑ Test teams should be identified early during development phase and test plans should be developed from development specifications. Test and development team leaders must communicate extensively.
- ❑ Test team leader should review test plan and test results with affected business area personnel.
- ❑ Initiate problem logs—Utilize effective problem identification and remediation tools to communicate problems, mitigation strategies and sign-

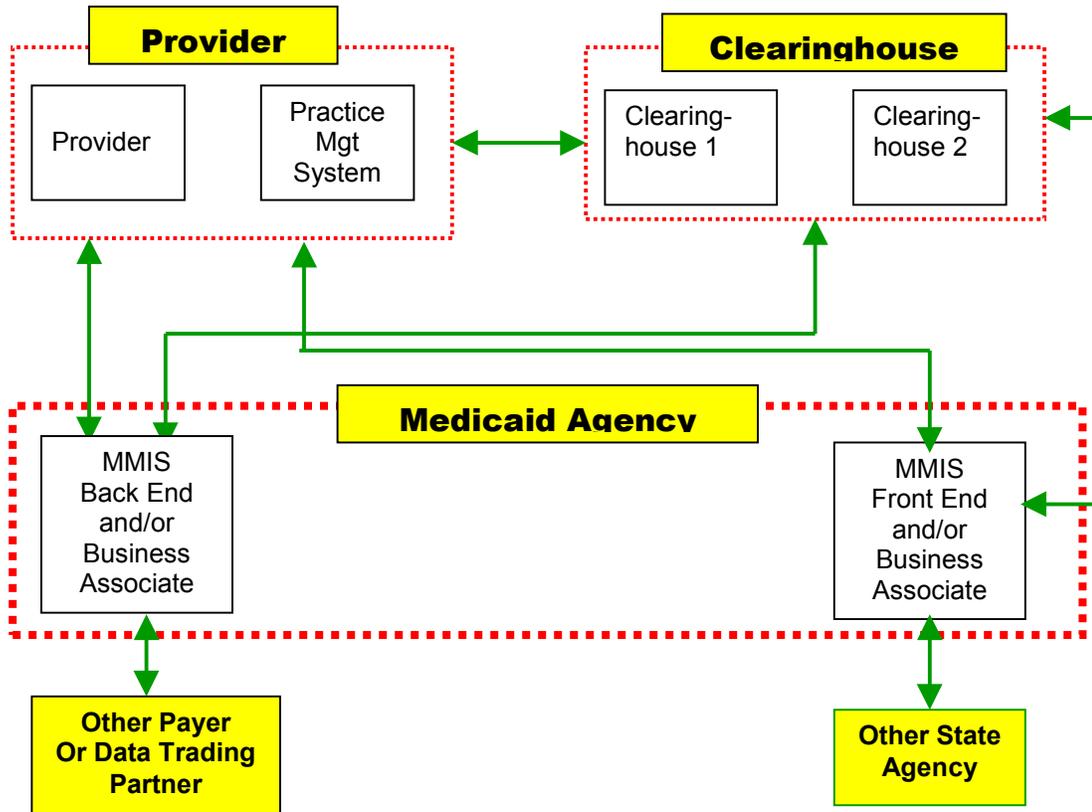
TESTING METHODOLOGY

off on fixes.

- ❑ Only promote changes when no more problems exist. Be ready to back out changes in the production environment when necessary.
- ❑ Review all user documentation and ensure they reflect changes that are now in place...Keep documentation current!

BUSINESS-TO-BUSINESS TESTING — (TEST ZONE 3)

The chart below shows a summary of all testing in a Fee-for-Service environment. The green (solid arrow lines) represent the business-to-business testing.



Green arrow = Business-to-Business Testing Zone 3 →

The above chart models the fee-for-service environment. Fee-for-service testing encompasses Claim/Encounter transactions, Eligibility Verification Request and Response, Claim Status Inquiry and Response, Prior Authorization Request and Response, Remittance Advice, and Coordination of Benefits. This model can be converted to a managed care view by replacing Providers with Managed Care Organizations. Transactions to be tested in the managed care environment are Enrollment, Premium Payment, Encounter Data, and Eligibility Verification.

Summary Of WEDI Business-to-Business Transaction Testing White Paper

The SNIP Transactions Work Group/Transaction Testing Sub Work Group has produced a white paper on *Business-to-Business Transaction Set Testing*³ that recommends solutions associated with transaction set testing between data exchange partners. The paper recommends the types of testing and establishes minimum levels of testing. Levels of testing appropriate to the business-to-business testing environment are proposed as follows:

- ❑ *Level 1: Transmission/File Integrity*—Test the transmission for completeness, valid segments, and segment order.
- ❑ *Level 2: Data Integrity*—Test for Implementation Guide required data elements and code values.
- ❑ *Level 3: Balancing*—Test for balanced field totals and record and segment counts. If a file fails any of the first three testing levels, it should be rejected as non-compliant. If an entity has been certified for compliance, the first three levels of testing can be shortened.
- ❑ *Level 4: Partner-Specific Business Scenario*—This is the core of the business-to-business testing program. Unlike the well-defined test requirements in the first three levels, these tests are more subjective, dependent on the nature of the data trading partners involved, and require boundary setting and buy-in from partners on both sides of the testing fence. The testing scenarios should include:
 - Conditional Situations: —Testing of specific, dependent situations where if one field is filled, other dependent situational fields must also be filled.
 - Code Sets: —This goes beyond the data integrity testing and focuses on the appropriate usage of the code.
 - Product Types or Types of Service: —This detailed level of testing focuses on the specific requirements of reporting related to the service, e.g., chiropractic, home health, nutrition, durable medical equipment, psychiatry, ambulance, and others.
 - Partner Data Validation: —Test for data values that are valid per the X12 format as specified in the Implementation Guide, but are not applicable to a particular data trading partner relationship. Verifies that the data from the standard transaction goes to the correct place in the receiver’s database.
 - Field Length: —Test for proper handling of X12 fields that are longer than the receiver’s system allows. The way the field is converted and truncated may make the data inaccurate.
 - Output: —Can output be produced as required by the receiver? For example, can the health plan produce both paper and electronic remittance advices?
- ❑ *Level 5: Load/Capacity/Volume*—Test to ensure that the systems of both partners will not fail because of increased file sizes. Related sizing factors to be tested include: batch run times, capacity of the translator, and other front-end programs.



³ See www.wedi.org Web site for the draft version of this paper.

- *Level 6: Security/Privacy*—With the option to delay one year in the transactions implementation, the Privacy Rule will go into effect first. It is important to start testing the files for Privacy and Security requirements. De-identification cannot be used for privacy at this point because that would block out data fields that are needed to test the integrity of the data. Appendix A of the WEDI paper contains a model test plan.

The State Medicaid agency should inform all members of its data trading community regarding its expectations for testing responsibility that lie outside of the agency. For example, providers and clearinghouses are covered entities with the same responsibility for compliance as the agency. Medicaid expects that all providers and clearinghouses will conduct their own compliance testing. Where possible, the covered entity should seek compliance certification. The following table presents some but not all of the business-to-business testing requirements.

BUSINESS-TO-BUSINESS TESTING DETAILS			
SENDER/RECEIVER	TRANSACTIONS	RESPONSIBLE COORDINATING PARTY	MINIMUM LEVEL OF TEST
Provider or practice management system (PMS) to Clearinghouse (CH)	Non standard transactions	Provider and CH: Both are covered entities.	Can CH produce HIPAA compliant transactions?
Clearinghouse 1 / Clearinghouse 2	All	Both	Can CH 1 exchange HIPAA compliant transactions with CH 2 and vice versa?
Provider or PMS, or managed care organizations (MCO) to MMIS Front End	837, 278, 276, 270 from providers and 270, 837 COB from health plans	Medicaid Agency	Can MMIS accept Provider's HIPAA compliant transactions?
CH 1 (= Provider or MCO partner) to MMIS Front End	All inbound transactions	Medicaid Agency	Can MMIS accept CH 1 HIPAA compliant transactions?
CH 2 (= Medicaid agency partner) to MMIS Front End	All inbound transactions	CH	Can MMIS accept CH 2 non-standard transactions?
MMIS Back End to CH 2 (CH = Medicaid agency partner)	All outbound transactions: 835, 271, 277, 278 for providers 834, 820, and 270 for health plans	CH	Can MMIS send non-standard transactions to CH for conversion to standard?
MMIS Back End to CH 1 (CH 1 = Provider/MCO partner)	All outbound transactions: 835, 271, 277, 278 for providers 834, 820, and 270 for health plans	Medicaid Agency	Can MMIS send standard transactions to CH?

BUSINESS-TO-BUSINESS TESTING DETAILS			
SENDER/RECEIVER	TRANSACTIONS	RESPONSIBLE COORDINATING PARTY	MINIMUM LEVEL OF TEST
MMIS Back End to Provider or MCO	All outbound transactions	Medicaid Agency	Can MMIS send standard transactions to provider?
Other State Agency to MMIS Front End	Departments of Health, Mental Health, Developmental Disabilities, et al: Waiver claims	Medicaid Agency	Can agency exchange standard transactions with other agency?
MMIS Back End to Other Payer or Data Trading Partner	COB MSIS input	Medicaid Agency	Can agency send 837 COB standard transaction to other payer?

Testing Parallel Pre-HIPAA/HIPAA-Compliant Systems

Even when all Business-to-Business testing is completed, additional testing is still required to ensure a smooth transition from pre-HIPAA functions to the new HIPAA-compliant system. It is unlikely that any State will plan to simultaneously switch over to all transactions on the deadline date of October 16, 2003. Each State will have a transition plan in which certain transactions can begin to be submitted in the new HIPAA format. However, the current processes will remain in place until the compliance deadline (or a prior agreed upon cut-over date) is reached. Given this scenario of managing parallel systems for some number of months, States must test the parallel outcomes to determine the accuracy of all functions. Parallel operations allow time to identify and fix problems with the business flow and outputs.

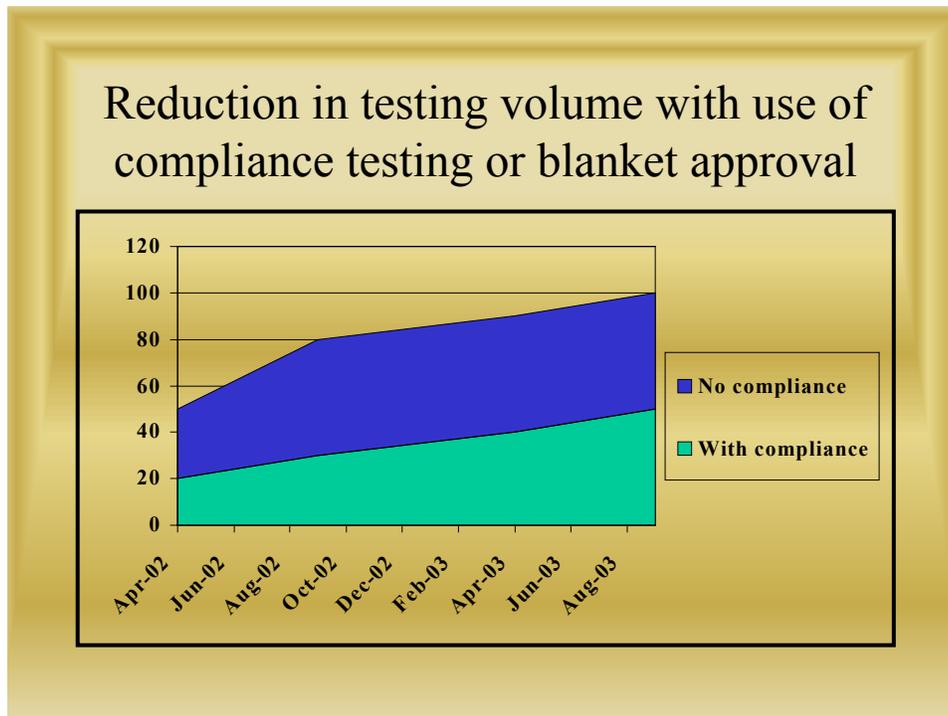
Blanket Approval

The Association For Electronic Health Care Transactions (AFEHCT) Medicare/Medicaid EDI Work Group proposed some testing shortcuts. To the extent that shared services and systems can be certified as compliant, the cost and time required for testing can be dramatically reduced. If the translator product is certified by a third party, or if some members of a billing group can pass a test, or if the clearinghouse has been certified, much time can be saved. Internal testing and Business-to-Business testing is still required, but many one-on-one tests can be eliminated. AFEHCT proposed a “blanket approval” approach as a shortcut for business-to-business testing. This approach applies to a Medicaid agency or a clearinghouse that receives transactions from multiple provider groups or individual providers who use a specific software vendor’s services to transmit the transaction. In a “blanket approval”⁴, there is a minimum number of providers who must transmit the transaction with a minimum number of errors in the batch. Acknowledgments must be successfully received. For example: “*At least five providers*

⁴AFEHCT, Medicare/Medicaid EDI Work Group, “*Summary of Proposed Language for HCFA EDI Support Manual*”, (Section on Provider Testing Requirements – “Blanket Approval”), December 1, 1997.

must transmit batches of 100 claims with less than 0.1% errors.” Blanket approval is given separately for each transaction.

Bringing together the staggering numbers of individual business-to-business tests and the prospect that “blanket approvals” and compliance certification testing could dramatically reduce these numbers and associated costs, we use the following table to illustrate the dilemma.



The above chart is not meant to suggest actual statistics and savings but to illustrate that whatever the impact, use of third party certification services and blanket approval approaches will reduce the overall volume of testing. Certification and blanket approval are associated with a point in time. Any change to a sender or receiver’s system may call for retesting.

The Sequencing Issue

What makes the whole Business-to-Business testing even more complicated is the issue of sequencing. If all entities were ready to test all transactions at the same time, there would still be a massive problem of planning the tests. But if all entities are focusing on different transactions at any point in time, there will be chaos! In response to the original deadline, WEDI SNIP proposed a national plan to sequence the transactions so that across the country, each entity would be testing the same transaction at the same time. The transaction grouping proposed by WEDI at that time is shown in the following table⁵:

⁵ See www.wedi.org for the white paper on *Sequencing*.

Schedule and Sequence Implementation Proposal

	Group 1	Group 2	Group 3	Group 4	Group 5
Transaction	837	270/271	276/277	278	820
Groups	835	834			

WEDI proposed three phases of implementation for each transaction set: Pilot Testing, Payer Readiness target date, and Final Implementation (the legal deadline). The WEDI message is that the health care data trading community needs to have a plan for transitioning from current processes to HIPAA compliant processes. The plan should encompass testing individual or groups of transactions according to a schedule that the data trading community agrees to. In some States providers may press for implementation of the standards prior to the deadline. To protect its interests, the Medicaid agency should communicate its implementation plans with the providers and seek legal advice regarding how to respond to requests to initiate testing by certain dates. If the Medicaid agency does not provide enough time for testing based on the providers' request, there could be legal ramifications.

Regional HIPAA Implementation Efforts

Local, statewide, and regional organizations have been formed both pre-HIPAA and recently to bring together payers and providers to foster communications and solve common problems. The WEDI/SNIP Education Committee created a HIPAA Regional Efforts Group charged with establishing a forum to unite the efforts of all regional groups. Coordination and cooperation are essential to the implementation of HIPAA. At present there are 35 States involved in regional SNIP efforts⁶. The SNIP Regional Efforts Group promotes development of the regional organizations and serves as a source for dissemination of information, tools, and materials⁷. SNIP has established a listserv for regional contacts at regional@wedi.org and has instituted conference calls. The work group is also currently conducting a "2001 Regional Efforts Implementation Survey" to identify successes and barriers in implementing HIPAA.

One of the key objectives of the Regional Efforts Group is to facilitate community-level compliance testing. After all, HIPAA will initially be implemented at the local level and not at the national level. Therefore collaboration among providers, payers, government agencies, professional associations, and business associates is essential. Regional organizations can apply to become a Regional SNIP Affiliate (RSA). It is hoped that a national network of RSAs can coordinate regional implementation plans at the local level. These plans will ensure the scheduling and timing of testing of groups of transactions.

⁶ Visit <http://snip.wedi.org/> for more information.

⁷ From a presentation by Ruth Tucci-Kaufhold, Co-Founder of the Mid-Atlantic Health Initiative (MAHI) at the National Managed Health Care Congress, January 8, 2002. See also <http://snip.wedi.org/>.

CONCLUSION

This paper has examined testing requirements at many levels and in key zones: translator product and application testing, internal Medicaid agency business application testing including testing with business associates, and Business-to-Business testing. Testing is a major part of transition planning. The primary message of the paper is that HIPAA implementation testing far exceeds any previous testing experience including Y2K in terms of breadth, volume, complexity, and numbers of required tests. Visit the WEDI/SNIP web site to view the papers on testing at <http://snip.wedi.org> (click on the Workgroups and Listservs link, then the Transactions Workgroup link, then the White Papers link).